JC07 Rec'd PCT/PTO 13 FEB 2002

Customized FORM PTO-1390 U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE

TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371

ATTORNEY DOCKET NO. P07532US90/MP

U.S. APPLICATION NO (known, see 37 CFR 1.5) 10/049529

INTERNATIONAL APPLICATION NO.	INTERNATIONAL FILING DATE	PRIORITY DATE CLAIMED
PCT/AU00/00972	11 AUGUST 2000	13 AUGUST 1999

TITLE OF INVENTION: USER AUTHENTICATION SYSTEM

APPLICANT(S) FOR DO/EO/US: TEFAYE, Joseph E.

Applicant herewith submits to the US Designated/Elected Office (DO/EO/US) the following items and other information:

☒ 1. This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.

☐ 2. This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 USC 371.

☒ 3. This express request to begin national examination procedures (35 USC 371(f)) at any time rather than delay examination until the expiration of the applicable time limit set in 35 USC 371(b) and PCT Art. 22 and 39(1).

☒ 4. A proper Demand for International Preliminary Examination was made by the 19th month from the earliest claimed priority date.

☒ 5. A **copy** of the International Application as filed (35 U.S.C. 371 (c)(2))
- ☐ a. is transmitted herewith (required only if not transmitted by the International Bureau).
- ☒ b. has been transmitted by the International Bureau.
- ☐ c. is not required, as the application was filed in the United States Receiving Office (RO/US).

☐ 6. A **translation** of the International Application into English (35 U.S.C. 371(c)(2)).

☒ 7. Amendments to the claims of the International Appln. under PCT Article 19 (35 USC 371 (c)(3))
- ☐ a. are transmitted herewith (required only if not transmitted by the International Bureau).
- ☐ b. have been transmitted by the International Bureau.
- ☐ c. have not been made; however, the time limit for making such amendments had NOT expired.
- ☒ d. have not been made and will not be made.

☐ 8. A translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(c)(3)).

☒ 9. An **oath** or declaration of the inventor(s) (35 U.S.C. 371(c)(4)).

☐ 10. A translation of the annexes to the Int'l Prelim. Exam. Report under PCT Article 36 (35 U.S.C. 371(c)(5)).

Items 11. to 20. below concern document(s) or information included:

☐ 11. An **Information Disclosure Statement** under 37 C.F.R. 1.97 and 1.98.

☐ 12. An **Assignment** document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included

☒ 13. A **First preliminary amendment.**

☐ 14. A Second or Subsequent preliminary amendment.

☐ 15. A substitute specification.

☐ 16. A change of power of attorney and/or address letter.

☐ 17. A computer-readable form of the sequence listing in accordance with PCT Rule 13ter.2 & 35 USC 1.821-825.

☐ 18. A second copy of the published international application under 35 USC 154(d)(4).

☐ 19. A second copy of the English translation of the international application under 35 USC 154(d)(4).

☐ 20. Other items or information:
- ☐
- ☐

☐ A copy of the Notification of Missing Requirements under 35 U.S.C. 371.

☐ In the event that a petition for extension of time is required to be submitted herewith, and in the event that a separate petition does not accompany this response, applicant hereby petitions under 37 CFR 1.136(a) for an extension of time of as many months as are required to render this submission timely. Any fee is authorized in 17(c).

Date: 13 Feb. 2002

U.S. APPLICATION NO. (if known)	INTERNATIONAL APPLICATION NO.	ATTORNEY DOCKET NO.
10/049529	PCT/AU00/00972	P07532US00/MP

☒ 21. **The following fees are submitted:**

CALCULATIONS *PTO USE ONLY*

☒ **Basic National Fee** (37 CFR 1.492 (a) (1)-(5):

☒	Neither Int'l Prelim. Exam. fee nor Int'l Search fee paid to USPTO	$1040
☐	Search Report has been prepared by the EPO or JPO	$ 890
☐	No Int'l Prelim. Ex. fee paid to USPTO but Int'l Search fee paid to USPTO	$ 740
☐	International preliminary examination fee paid to USPTPO	$ 710
☐	Int'l Prelim. Ex. fee paid to USPTO & all claims satisfied PCT Art. 33(1)-(4)	$ 100

			ENTER APPROPRIATE BASIC FEE AMOUNT =	$ 1040	
☐	Surcharge of **$130** for furnishing the oath or declaration later than from the earliest claimed priority date (37 CFR 1.492(e)).		☐ 20 mos. ☐ 30 mos. +	$	
CLAIMS	*NUMBER FILED*	*NUMBER EXTRA*	*RATE*		
Total Claims	32 - 20 =	02	X **$18** =	$ 36	
Independent Claims	04 - 03 =	01	X **$84** =	$ 84	
☐	Multiple Dependent Claim(s) (if applicable)		+ **$280** =	$	
			TOTAL OF ABOVE CALCULATIONS =	$ 1160	
☒	Applicant claims small entity status. See 37 CFR 1.27. The fees indicated above are reduced by ½.		-	$ 580	
			SUBTOTAL =	$ 580	
☐	Processing fee of **$130** for furnishing the **English translation** later than from the earliest claimed priority date (37 CFR 1 492(f)).		☐ 20 mos. ☐ 30 mos. +	$	
			TOTAL NATIONAL FEE =	$ 580	
☐	Fee for recording the enclosed **assignment** (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31). **$40** per property		+	$	
			TOTAL FEES ENCLOSED =	$ 580	
			Amount to be	*Refunded*	$
				Charged	$

☒ a. A **check** in the amount of $580.00 to cover the above fees is enclosed.

☐ b. Please charge my Deposit Account No. 12-0555 in the amount of $ to cover the above fees.

☒ c. The Commissioner is hereby authorized to charge any additional fees required or credit overpayment to Deposit Account No. 12-0555.

Note: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and granted to restore the application to pending status.

SEND ALL CORRESPONDENCE TO:

MARVIN PETRY

At the address (below) of **CUSTOMER NO. 00881.**

LARSON & TAYLOR, PLC
1199 NORTH FAIRFAX ST.
SUITE 900
ALEXANDRIA, VA 22314

SIGNATURE: Douglas E. Jackson

NAME: Douglas E. Jackson

REG. NO.: 28518

PHONE NO.: 703-739-4900

Date: 13 Feb. 2002

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Patent

In re patent application of: TEFAYE

Serial No.: Unassigned — Examiner: Unassigned

Filed: On even date herewith — Art Unit: Unassigned

For: USER AUTHENTICATION SYSTEM — Dckt No.: P07532US00

PRELIMINARY AMENDMENT

Assistant Commissioner of Patents

Washington, D.C. 20231

SIR:

Prior to examination, please amend the above-identified application as follows:

IN THE CLAIMS

Cancel claims 33-35.

A clean version of all pending claims is provided herewith in **Attachment A**. It will be noted that claims 3, 6-8, 10-15, 19-21, and 23-29 have been amended relative to the previously provided version as shown by the marked up version thereof in **Attachment B** provided herewith.

REMARKS

The present amendment is made to eliminate multiple dependent claims and thus eliminate the requirement for a multiple claim fee.

Respectfully submitted,

Date: 2/13/02

Douglas E. Jackson

By: Douglas E. Jackson
Registration No.: 28,518

LARSON & TAYLOR, PLC • 1199 North Fairfax St. • Suite 900 • Alexandria, VA 22314 • (703) 739-4900

ATTACHMENT A

Clean Replacement/New Claims (entire set of pending claims)

Following herewith is a clean copy of the entire set of pending claims.

1. A user authentication method to authenticate a registered user of a service over a computer network, the method comprising the steps of:

(a) permitting a client user to request a service from a service provider accessible from said computer network;

(b) requiring the client user to submit at least one first password to the service provider;

(c) requiring the client user to submit at least one unique graphic to the service provider, said unique graphic including embedded second password data;

(d) extracting the second password from said embedded second password data contained within said unique graphic;

(e) comparing the submitted first password and extracted second password to determine if a pre-defined relationship exist between the passwords; and

(f) granting the client user authentic registered user status if said pre-defined relationship exist and providing access to said service.

2. A user authentication method as claimed in claim 1, said method further comprising the steps of:

(h) allowing a registered user of said service to select said first password.

3. (amended) A user authentication method as claimed in claim 1, said method further comprising the step of:

(i) allowing said user to select an input value;

(j) using said selected input number to index a table to determine a table number; and

(k) using the table number to determine an output number and thereby the second password.

4. A user authentication method as claimed in claim 3, wherein said method comprises the step of randomly mapping input values with output values.

5. A user authentication method as claimed in claim 2, said step (h) further comprising the step of:

(i) issuing said second password once the registered user has selected said first password, said second password issued according to said pre-defined relationship.

6. (amended) A user authentication method as claimed in claim 1, wherein said predefined relationship is determined according to the formula:

$$y=x$$

wherein, y is said first password and x is said second password.

7. (amended) A user authentication method as claimed in claim 1, wherein said pre-defined relationship is determined according to the formula:

$$y=mx$$

wherein said passwords are numerical and y is said first password, x is said second password and m is a constant.

8. (amended) A user authentication method as claimed in claim 1, wherein said pre-defined relationship is determined according to the formula:

$$y=mx + c$$

wherein said passwords are numerical and y is said password, x is said second password and m and c are constant.

9. A user authentication method as claimed in claim 2, wherein in step (h), said registered user selects on or more calendar dates as a password and step (h) further comprises the step of:

(i) issuing a random number associated with said selected one or more calendar dates and using said random number to identify said registered user.

clean claims

10. (amended) A user authentication method as claimed in claim 1, wherein said service relates to credit card payment facilities or electronic mail services.

11. (amended) A user authentication method as claimed in claim 1, wherein said service provider is a credit card payment authorization service.

12. (amended) A user authentication method as claimed in claim 1, wherein said unique graphic is a fractal.

13. (amended) A user authentication method as claimed in claim 10, wherein said fractal is drawn according to a Mandlebrot set according to the set of values of C for the series $Z_{N+1} = (Z_N)^2+C$.

14. (amended) A user authentication method as claimed in claim 1, wherein date time stamp data is issued to a registered user when they are issued with the unique graphic and this date time stamp is embedded within said unique graphic.

15. (amended) A user authentication method as claimed in claim 1, wherein a transaction number is issued to the registered user for each service request that is granted over the computer network.

16. A user authentication system to authenticate a registered user of a service over a communication network, the authentication system comprising:

service means connected to said communications network having one or more information pages associated with a service provider;

a client device adapted to interface with said server means via said communication network, said client device capable of accessing said one or more information pages to thereby permit said user to submit at least one first password and at least one unique graphic comprising embedded second password data, to the service provider via said one or more information pages, and

clean claims

authentication means adapted to interface with said server means to thereby extract the second password from the embedded second password data contained within the unique graphic, and compare the submitted first password and extracted second password to determine if a pre-defined relationship exists between the passwords,

wherein in use, the user is granted registered user status and is allowed access to said service if said pre-defined relationship exists.

17. A user authentication system as claimed in claim 16, wherein said authentication means allows a registered user of said service to select said first password.

18. A user authentication system as claimed in claim 17, wherein said second password is issued once the registered user has selected said first password, and said second password is issued according to said pre-defined relationship.

19. (amended) A user authentication system as claimed in claim 16, wherein said pre-defined relationship is determined according to the formula:

$$y=x$$

wherein, y is said first password and x is said second password.

20. (amended) A user authentication system as claimed in claim 16, wherein pre-defined relationship is determined according to the formula:

$$y=mx$$

wherein said passwords are numerical and y is said first password, x is said second password and m is a constant.

21. (amended) A user authentication system as claimed in claim 16, wherein said pre-defined relationship is determined according to formula:

$$y=mx+c$$

wherein said passwords are numerical and y is said first password, x is said password and m and c are constant.

clean claims

22. A user authentication system as claimed in claim 17, wherein said registered user selects one or more calendar dates as a password and a random number is issued that is associated with said selected one or more calendar dates, said random number being used to identify said registered user.

23. (amended) A user authentication system as claimed in claim 16, wherein said service relates to credit card payment facilities or electronic mail services.

24. (amended) A user authentication system as claimed in claim 16, wherein said service provider is a credit card payment authorization service.

25. (amended) A user authentication system as claimed in claim 16, wherein said unique graphic is a fractal.

26. (amended) A user authentication system as claimed in claim 25, wherein said fractal is drawn according to a Mandlebrot set according to the set of values of C for the series $Z_{N+1}=(Z_N)^2+C$.

27. (amended) A user authentication system as claimed in claim 16, wherein date time stamp data is issued to a registered user when they are issued with the unique graphic and this date time stamp is embedded within said unique graphic.

28. (amended) A user authentication system as claimed in claim 16, wherein a transaction number is issued to the registered user for each service request that is granted over the computer network.

29. (amended) A user authentication system as claimed in claim 16, wherein said user to selects an input value and uses said selected input number to index a table to determine a table number, and using the table number to determine an output number and thereby the second password.

30. A user authentication system as claimed in claim 29, wherein said system further comprises randomly mapping input values with output values.

31. A user authentication system to authenticate a registered user of a credit card service on an Internet environment, the authentication system comprising;

server connected to the Internet having one or more web pages associated with said vendor, said vendor web pages permitting purchase of goods/services therefrom;

a client device operable by a user, said client device adapted to connect to said service via the Internet and download one or more of said web pages, said client user being thereby permitted to submit a first password and, a unique graphic including an embedded second password, to the service provider via said web pages; and

authentication software adapted to interface with said server to thereby extract the second password from the unique graphic and compare the submitted first password and second password to determine if a pre-defined relationship exists between the passwords,

wherein in use, the client user is granted registered user status and is allowed access to said credit card service if said pre-defined relationship exists.

32. A user authentication method to authenticate a registered user of a service over a computer network, the method comprising the steps of:

(a) permitting a client user to request a service form a service provider accessible from said computer network;

(b) requiring the client user to submit a unique graphic to the service provider;

(c) comparing said submitted unique graphic with a unique graphic pre-recorded with said service provider to determine if they are the same; and

(d) granting the client user registered user status if said submitted unique graphic is the same as said unique graphic pre-recorded with said service provider and thereby providing access to said service from said computer network.

ATTACHMENT B

Marked Up Replacement Claims

Following herewith is a marked up copy of each rewritten claim together with all other pending claims.

1. A user authentication method to authenticate a registered user of a service over a computer network, the method comprising the steps of:

(a) permitting a client user to request a service from a service provider accessible from said computer network;

(b) requiring the client user to submit at least one first password to the service provider;

(c) requiring the client user to submit at least one unique graphic to the service provider, said unique graphic including embedded second password data;

(d) extracting the second password from said embedded second password data contained within said unique graphic;

(e) comparing the submitted first password and extracted second password to determine if a pre-defined relationship exist between the passwords; and

(f) granting the client user authentic registered user status if said pre-defined relationship exist and providing access to said service.

2. A user authentication method as claimed in claim 1, said method further comprising the steps of:

(h) allowing a registered user of said service to select said first password.

3. (amended) A user authentication method as claimed in claim 1 ~~or claim 2~~, said method further comprising the step of:

(i) allowing said user to select an input value;

(j) using said selected input number to index a table to determine a table number; and

(k) using the table number to determine an output number and thereby the second password.

4. A user authentication method as claimed in claim 3, wherein said method comprises the step of randomly mapping input values with output values.

5. A user authentication method as claimed in claim 2, said step (h) further comprising the step of:

(i) issuing said second password once the registered user has selected said first password, said second password issued according to said pre-defined relationship.

6. (amended) A user authentication method as claimed in ~~one of the preceding~~ claims 1, wherein said predefined relationship is determined according to the formula:

$$y=x$$

wherein, y is said first password and x is said second password.

7. (amended) A user authentication method as claimed in ~~any one of~~ claims ~~1 to~~ 4, wherein said pre-defined relationship is determined according to the formula:

$$y=mx$$

wherein said passwords are numerical and y is said first password, x is said second password and m is a constant.

8. (amended) A user authentication method as claimed in ~~any one of~~ claims ~~1 to~~ 4, wherein said pre-defined relationship is determined according to the formula:

$$y=mx + c$$

wherein said passwords are numerical and y is said password, x is said second password and m and c are constant.

9. A user authentication method as claimed in claim 2, wherein in step (h), said registered user selects on or more calendar dates as a password and step (h) further comprises the step of:

(i) issuing a random number associated with said selected one or more calendar dates and using said random number to identify said registered user.

marked claims

10. (amended) A user authentication method as claimed in ~~any one of the above~~ claims 1, wherein said service relates to credit card payment facilities or electronic mail services.

11. (amended) A user authentication method as claimed in ~~any one of the above~~ claims 1, wherein said service provider is a credit card payment ~~autherisation~~authorization service.

12. (amended) A user authentication method as claimed in ~~any one of the above~~ claims 1, wherein said unique graphic is a fractal.

13. (amended) A user authentication method as claimed in claim 10, wherein said fractal is drawn according to a Mandlebrot set according to the set of values of C for ~~which~~ the series $Z_{N+1} = (Z_N)^2+C$.

14. (amended) A user authentication method as claimed in ~~any one of the above~~ claims 1, wherein date time stamp data is issued to a registered user when they are issued with the unique graphic and this date time stamp is embedded within said unique graphic.

15. (amended) A user authentication method as claimed in ~~any one of the above~~ claims 1, wherein a transaction number is issued to the registered user for each service request that is granted over the computer network.

16. A user authentication system to authenticate a registered user of a service over a communication network, the authentication system comprising:

service means connected to said communications network having one or more information pages associated with a service provider;

a client device adapted to interface with said server means via said communication network, said client device capable of accessing said one or more

marked claims

information pages to thereby permit said user to submit at least one first password and at least one unique graphic comprising embedded second password data, to the service provider via said one or more information pages, and

authentication means adapted to interface with said server means to thereby extract the second password from the embedded second password data contained within the unique graphic, and compare the submitted first password and extracted second password to determine if a pre-defined relationship exists between the passwords,

wherein in use, the user is granted registered user status and is allowed access to said service if said pre-defined relationship exists.

17. A user authentication system as claimed in claim 16, wherein said authentication means allows a registered user of said service to select said first password.

18. A user authentication system as claimed in claim 17, wherein said second password is issued once the registered user has selected said first password, and said second password is issued according to said pre-defined relationship.

19. (amended) A user authentication system as claimed in ~~any one of~~ claims ~~16 to 18~~, wherein said pre-defined relationship is determined according to the formula:

$$y=x$$

wherein, y is said first password and x is said second password.

20. (amended) A user authentication system as claimed in ~~any one of~~ claims ~~16 to 18~~, wherein pre-defined relationship is determined according to the formula:

$$y=mx$$

wherein said passwords are numerical and y is said first password, x is said second password and m is a constant.

21. (amended) A user authentication system as claimed in ~~any one of~~ claims ~~16 to 18~~, wherein said pre-defined relationship is determined according to formula:

marked claims

y=mx+c

wherein said passwords are numerical and y is said first password, x is said password and m and c are constant.

22. A user authentication system as claimed in claim 17, wherein said registered user selects one or more calendar dates as a password and a random number is issued that is associated with said selected one or more calendar dates, said random number being used to identify said registered user.

23. (amended) A user authentication system as claimed in ~~any one of~~ claim~~s~~ 16~~ to 22~~, wherein said service relates to credit card payment facilities or electronic mail services.

24. (amended) A user authentication system as claimed in ~~any one of~~ claim~~s~~ 16~~ to 23~~, wherein said service provider is a credit card payment ~~autherisation~~authorization service.

25. (amended) A user authentication system as claimed in ~~any one of~~ claim~~s~~ 16~~ to 24~~, wherein said unique graphic is a fractal.

26. (amended) A user authentication system as claimed in claim 25, wherein said fractal is drawn according to a Mandlebrot set according to the set of values of C for ~~which~~ the series $Z_{N+1}=(Z_N)^2+C$.

27. (amended) A user authentication system as claimed in ~~any one of~~ claim~~s~~ 16~~ to 26~~, wherein date time stamp data is issued to a registered user when they are issued with the unique graphic and this date time stamp is embedded within said unique graphic.

28. (amended) A user authentication system as claimed in ~~any one of~~ claim~~s~~ 16~~ to 27~~, wherein a transaction number is issued to the registered user for each service request that is granted over the computer network.

29. (amended) A user authentication system as claimed in claim 16 ~~or claim 17~~, wherein said user to selects an input value and uses said selected input number to index a table to determine a table number, and using the table number to determine an output number and thereby the second password.

30. A user authentication system as claimed in claim 29, wherein said system further comprises randomly mapping input values with output values.

31. A user authentication system to authenticate a registered user of a credit card service on an Internet environment, the authentication system comprising;

server connected to the Internet having one or more web pages associated with said vendor, said vendor web pages permitting purchase of goods/services therefrom;

a client device operable by a user, said client device adapted to connect to said service via the Internet and download one or more of said web pages, said client user being thereby permitted to submit a first password and, a unique graphic including an embedded second password, to the service provider via said web pages; and

authentication software adapted to interface with said server to thereby extract the second password from the unique graphic and compare the submitted first password and second password to determine if a pre-defined relationship exists between the passwords,

wherein in use, the client user is granted registered user status and is allowed access to said credit card service if said pre-defined relationship exists.

32. A user authentication method to authenticate a registered user of a service over a computer network, the method comprising the steps of:

(a) permitting a client user to request a service form a service provider accessible from said computer network;

(b) requiring the client user to submit a unique graphic to the service provider;

(c) comparing said submitted unique graphic with a unique graphic pre-recorded with said service provider to determine if they are the same; and

(d) granting the client user registered user status if said submitted unique graphic is the same as said unique graphic pre-recorded with said service provider and thereby providing access to said service from said computer network.

marked claims

User authentication system

Field of the invention

The present invention relates to a user authentication system on a computer network such as the Internet and to a method of implementing same.

Background of the invention

The Internet is rapidly changing the way the world communicates and conducts business. There continues to be an exponential increase in the number of users who gain access to the Internet and who subsequently wish to purchase goods and services via this medium.

While the potential market for businesses offering goods and services over the Internet is enormous due to the large number of websites and ease of access to users, a perception amongst a number of Internet users is that information passed over the Internet is not particularly secure as it can be intercepted by other Internet users and more particularly hackers. To circumvent this, a number of web sites operators enhance their web sites by encrypting data over the Internet transport layer.

Although the actual transmission between a web vendor and a customer over the web may be relatively secure, there is nothing to prevent an unscrupulous person from copying the customer's credit card number and expiry date and then using this information to purchase goods from a website. The web vendors do not perform a check to determine if the person making the purchase is the actual credit card holder, they simply check with the credit card issuing body as to whether the card is valid, they confirm the expiry date of the credit card and that there are sufficient funds on the account to make the purchase.

The applicant does not concede that the prior art discussed in this specification forms part of the common general knowledge in the art at the priority date of this application.

Summary of the invention

It is an object of the invention to provide an advantageous user authentication system and method of implementing same.

According to a first aspect of the present invention, there is provided a user authentication method to authenticate a registered user of a service over a computer network, the method comprising the steps of:

(a) permitting a client user to request a service from a service provider having one or more information pages accessible from said computer network;

(b) requiring the client user to submit a first password via said one or more information pages to the service provider;

(c) requiring the client user to submit a unique graphic via said one or more information pages to the service provider, said unique graphic including embedded second password data;

(d) extracting the second password from said embedded second password data contained within said unique graphic;

(e) comparing the submitted first password and extracted second password to determine if a pre-defined relationship exists between the passwords; and

(f) granting the client user authentic registered user status if said pre-defined relationship exists and providing access to said service.

The method may further comprise the step of:

(h) allowing a registered user of said service to select said first password. Further, step (h) may further comprise the step of:

(i) issuing said second password once the registered user has selected said first password, said second password issued according to said pre-defined relationship.

Optionally, said method further comprising the step of:

(i) allowing said user to select an input value;

(j) using said selected input number to index a table to determine a table number; and

(k) using the table number to determine an output number and thereby the second password.

The method may also comprise the step of randomly mapping input values with output values.

The pre-defined relationship may be determined according to the formula:

$$y = x$$

wherein, y is said first password and x is said second password.

The pre-defined relationship may be determined according to the formula:

$$y = mx$$

wherein said passwords are numerical and y is said first password, x is said second password and m is a constant.

The pre-defined relationship may be determined according to the formula:

$$y = mx + c$$

wherein said passwords are numerical and y is said first password, x is said second password and m and c are constant.

In step (h), said registered user may select one or more calendar dates as a password and step (h) may further comprise the step of:

(i) issuing a random number associated with said selected one or more calendar dates and using said random number to identify said registered user.

The service may relate to credit card payment facilities.

The service provider may be a credit card payment authorisation service.

The unique graphic may be a fractal and preferably is drawn according to a Mandlebrot set according to the set of values of C for which the series $Z_{N+1} = (Z_N)^2 + C$ converges, wherein Z and C are determined for each user according to a predefined algorithmic variation of two particular pieces of information, one for Z and one for C. For example, Z and C may be based on a number unique to the user such as their Driver's License or Social Security number, Medicare Card. With such a nominated number as input, the values of Z and C can optionally be calculated according to a formula.

A date time stamp data may be issued to a registered user when they are issued with the unique graphic and this date time stamp is embedded within said unique graphic.

A transaction number may be issued to the registered user for each service request that is granted over the computer network.

According to another aspect of the present invention, there is provided a user authentication system to authenticate a registered user of a service over a communication network, the authentication system comprising:

server means connected to said communications network having one or more information pages associated with a service provider;

a client device adapted to interface with said server means via said communication network, said client device capable of accessing said one or more information pages to thereby permit said user to submit a first password and a unique graphic comprising embedded second password data, to the service provider via said one or more information pages; and

authentication means adapted to interface with said server means to thereby extract the second password from the embedded second password data contained within the unique graphic, and compare the submitted first password and extracted second password to determine if a pre-defined relationship exists between the passwords,

wherein in use, the client user is granted registered user status and is allowed access to said service if said pre-defined relationship exists.

According to yet another aspect of the present invention, there is provided a user authentication system to authenticate a registered user of a credit card service in an Internet environment, the authentication system comprising:

server connected to the Internet having one or more web pages associated with said vendor, said vendor web pages permitting purchase of goods/services therefrom;

a client device operable by a user, said client device adapted to connect to said server via the Internet and download one or more of said web pages, said client user being thereby permitted to submit a first

password and, a unique graphic including an embedded second password, to the service provider via said web pages; and

authentication software adapted to interface with said server to thereby extract the second password from the unique graphic and compare the submitted first password and second password to determine if a pre-defined relationship exists between the passwords,

wherein in use, the client user is granted registered user status and is allowed access to said credit card service if said pre-defined relationship exists.

According to another aspect of the present invention, there is provided a user authentication method to authenticate a registered user of a service over a computer network, the method comprising the steps of:

(a) permitting a client user to request a service from a service provider accessible from said computer network;

(b) requiring the client user to submit a unique graphic to the service provider;

(c) comparing said submitted unique graphic with a unique graphic pre-recorded with said service provider to determine if they are the same; and

(d) granting the client user registered user status if said submitted unique graphic is the same as said unique graphic pre-recorded with said service provider and thereby providing access to said service from said computer network.

In the description and claims of this specification the word "comprise" and variations of that word, such as "comprises" and "comprising" are not intended to exclude other features, additives, components, integers or steps but rather, unless otherwise stated explicitly, the scope of these words should be construed broadly such that they have an inclusive meaning rather than an exclusive one.

Brief description of the drawings

Notwithstanding any other forms which may fall within the scope of the present invention, preferred forms of the invention will now be described, by way of example only, with reference to the accompanying drawings in which:

Fig 1 is a schematic illustration of a preferred system to authenticate a registered user of a credit card service;

Fig 1A is a display of a virtual form from a web page that a credit card user completes to obtain registration with the credit card authentication service;

Fig 1B is a display of an email that is sent to a user once they have registered for the credit card authentication service;

Fig 2 is of a display of a virtual form from a vendor website which is downloaded by a client computer and viewed from the client's web browser software;

Fig 3 is a schematic illustration of a Birth Date chart used in the preferred embodiment;

Fig 3A is a schematic illustration of the fields associated with a credit card holders details recorded in the data base of the credit card authentication service of Fig. 1;

Fig 4 is a schematic illustration of the steps which are involved in authenticating a credit card purchase from the credit card authentication service of Fig. 1;

Fig 5 is a schematic illustration of the virtual form of Fig 2 after an authentication check has determined that the purchase request is from a registered user of the credit card authentication service;

Fig 6 is a schematic illustration of the virtual form of Fig 2 after a authentication check has determined that the purchase is not from a registered user of the credit card authentication service and therefore the purchase has been denied; and

Fig. 7 is a schematic illustration of how passwords are extracted and compared by the system of Fig. 1.

Detailed description of the embodiments

A preferred embodiment provides an authentication method and system to authenticate a registered user of a credit card service in an Internet environment. The authentication system includes a server which is connected to the Internet and from which any number of web pages associated with an Internet vendor is available for the purchase of goods and services. When a personal computer connects to the Internet and downloads one of the web pages, the user submits a purchase request which includes a first password and a graphic file having embedded password data when they wish to make a purchase request from the vendor. The purchase request information sent to the vendor is routed to a server having authentication software which extracts the password data embedded in the graphic file and compares this with the first password. If a pre-defined relationship exists between the two passwords, the authentication software grants registered user status to the purchase request and the purchase is allowed to proceed.

Referring now to Fig 1, there is shown a schematic illustration of a user authentication system 10 for a credit card service. The user authentication system 10 includes a Credit Card Authentication Centre (CCAC) 15 which includes a server 14 which is connected to the Internet 12. The server 14 further includes a database 16 on which credit card information for a multiplicity of registered users is stored. The credit card information includes registered user contact details, authentication data and the actual credit card details.

In addition to the database, the server 14 also includes authentication software 18 for authenticating credit card data. The authentication software 18 further includes random number software 20 in the form of a birth date chart comprising a table of random numbers as will also be described in detail below.

A web site 21 is also accessible from the server 14 and is written in HTML code. The web site 21 is used to register users in the data base 16 and to permit a registered user to change their contact details as required.

The authentication system 10 may further include a number of Internet vendors 23, 25 who operate respective web sites 26, 28. The web sites 26, 28 are Internet vendor web sites which offer goods and services to

customers when the respective servers 22 and 24 are accessed via the Internet 12. Although only two web site vendors are shown in Fig 1, it should be understood that this is for illustrative purposes only and that any number of web site vendors could participate in the system.

Each of the website vendors 23 and 25, participate in the user authentication system to determine whether a person using a credit card via their website is in fact a registered user of the CCAC 15.

A plurality of client computers 30...31 are shown which can access the Internet 12 via their ISP (not shown). In this example, client user 30 is a registered user of the CCAC 15 and client user 31 is not a registered user of the CCAC 15 system. To register with the CCAC 15, the client user downloads the Credit Card Authentication Registration form 43 shown in Fig 1A, from the web site 21. As can be seen in this diagram, the client user, Joe Citizen, enters his contact details, shown generally by arrow 44, in addition to:

(1) his credit card number 45;

(2) his credit card issuing company, Mastercard 46;

(3) the expiry date of his credit card 47;

The user is then prompted for:

(1) a first birth date 48, preferably not the user's own and one that he will readily remember (in this case, 1 January);

(2) a second birth date 48', (31 December); and

(3) a two digit number 48'', (in this case 10).

This two digit number 48'' is used to create a unique graphic identifier (**UGI**) which is later issued to the user by the CCAC 15 system.

Once the form 43 is completed, the client user 30 then sends the information contained within the of form 43 to the server 14 by clicking the SUBMIT button. Should the client user not wish to proceed with registration, they click the CANCEL button.

In an alternative embodiment, the user could also input his/her credit card PIN number for authentication of the credit card as being properly registered with the CCAC 15. Another alternative to the user inputting a two digit number in field 48'' may involve the user inputting a number associated with his/her person, such as a drivers licence number, Medicare number, Social Security number etc. This number can then be input into a pre-defined formula and a number derived to draw the UGI as will be explained below.

Upon receiving the registration data referred to above, the authentication program reads the two digit number "10" selected by the client in field 48''. This number is used to generate a UGI. The UGI is preferably a fractal and more preferably is generated according to the Mandlebrot set:

$$Z_{N+1} = (Z_N)^2 + C$$

series of numbers where, where in Z and C are determined for each user according to a predefined algorithmic variation of two particular pieces of information, one for Z and one for C. For example, Z is calculated by taking the number from field 48'' and then using this number to calculate an initial value of Z and C, such as, where field 48'' is M = 10 and the first birth date field 48 is N= 0101, the initial value of Z and C could be:

$$Z_o = 0.6M^{1/2}$$

$$= 0.6(10)^{1/2}$$

$$= 1.89$$

and

$$C = 0.4N^{1/3}$$

$$= 0.4(101)^{1/3}$$

$$= 1.86$$

The authentication program then reads the two dates 48, 48' and sets a first password for the registered user as 01013112, being the two dates selected in form 43 of Fig. 1A.

When the client user 30 is registered as a user of the CCAC 15, the authentication software 18 records the date and time of when registration is issued to the client 30 and a Date Stamp is generated for the registered user. This assists the CCAC 15 from distinguishing from different users of the CCAC 15 who have the same name, or the one registered user who has a number of credit cards registered with the service. In this example, the registration was issued on 13 August 1999 at 3:03.25 PM, therefore the Date Stamp issued for the registration of this example is: "130899-150325"1.

Once the first password is recorded in the database, the random number software 20 which is a part of the authentication software 18, generates a routine to assign a random number value related to the input password. In this example, the random number value relates to the Birth Day Chart 32, are shown in Fig 3. The birthday chart 32 is a chart listing the dates of the sequential days of the year as shown in the birth date column 54, and having a corresponding assigned value called the UGI number shown in column 56.

It will be appreciated that the numbers for the dates of the year are sequential in this diagram, but this is for illustrative purposes only and that the preferred form involves a randomly assigned series of dates of the year in column 54. Furthermore the Birth Day chart is only preferable and it should be realised that any random number sequence could be used, such as choosing a star sign and then associating a UGI number with that star sign.

The UGI number in the Birth Date chart has UGI No's 1 to 365 and is associated with respective calendar dates 1/1 to 31/12 (this example does not relate to a leap year). Therefore, as the user in Fig 1A, has selected the birth date 0101 and 3112, they are assigned UGI number 1, and 365. The UGI numbers could be used to also generate the UGI graphic in other embodiments without having the client user select the field 48'' as shown in Fig 1A.

Optionally once the client user 30 has been assigned the unique UGI numbers 1, 365, these details are recorded in the database 16.

Once the UGI has been generated according to the number input by the user in field 48'' of Fig 1B, the UGI data is broken down into binary format and the UGI No, 1 and 365, are formatted into binary format from an ASCII text character to binary format. The UGI Numbers are then embedded within the binary data of the UGI. Once the client user 30 is registered as a user of the CCAC 15, the authentication program then sends an encrypted email as shown in Fig. 1B. The email confirms the registration and provides the client user 30 with the first password (01013112) and the UGI graphic which includes the embedded UGI numbers 1 and 365. Alternatively, the first password could be communicated verbally over the phone to the client user 30 or alternatively could be sent via the postal service for added security so that both first password and UGI are not sent in the same communication. Furthermore, it should also be understood that the actual UGI shown in Fig. 1B is shown as an example of a UGI and is not a UGI determined according to the formula above.

The data associated with the registered user Joe Citizen which is recorded in the CCAC 15 database 16, is shown in Fig 3A, including the Date Stamp 130899-150325 referred to above.

When a client user 30 wishes to purchase a product from an Internet vendor such as vendor 23 who operates website 26, they typically select the product and download an order form page, an example of which is shown in Fig 2. In this example, the client user wishes to purchase 'Book X' for $89.95 (refer to field 38). The virtual form 32, has a number of fields which the client user 30 enters, such as title, first name, last name, address, suburb, postcode, state, country etc. The user also enters their credit card number into field 34, the expiry date of their credit card in field 36, the purchase amount in field 38, their eight digit designated password '01013112' (field 40) and their designated UGI with embedded UGI number in field 44. Typically the UGI is copied from the client 30 and pasted in the Internet browser application in field 44. In other embodiments, this may be executed automatically by a suitably .exe program.

Once the user has completed the purchase request form as shown in Fig. 2, the user selects the submit button which sends the information to the server 22. Upon receiving this information, before the transaction can proceed, the website server 22 automatically routes the purchase request information including the UGI from field 44 and the eight digit password from filed 40 to the CCAC 15 server 14.

Upon receipt of the purchase request by the server 14, the authentication program 18 then begins the process of authenticating the user. Firstly, the UGI is decrypted by the authentication software 18 and extracts according to an encryption key, UGI numbers encrypted within the UGI which are recorded as UGI#1 and UGI#2. In this example, UGI#1 = 1 and UGI#2 = 365. The authentication program 18 refers to the random number software 20 having the Birth Date chart table 52 shown in Fig. 3, to obtain the respective corresponding birth dates.

In this example, the corresponding birth date to UGI#1 is 0101 and this birth date is assigned as variable P3 and as the corresponding UGI#2 = 3112, the birth date is for UGI#2 is assigned as variable P4.

Once the variables P3 and P4 have been assigned, the authentication software 18 reads the password 01013112 input into field 40 of the Fig. 2, and reads the first four characters of the password and stores this as P1.

It then reads the second four digits of the password and stores this as P2. Hence P1 = 0101 and P2 = 3112. The authentication software 18 then determines if the person making the purchase request is a registered user of the CCAC 15 by determining if there is a pre-defined relationship. In this embodiment if:

$$P1 = P3$$

$$P1 - P3 = 0$$

and

$$P2 = P4$$

$$P2 - P4 = 0$$

then the person making the purchase request is granted user access rights.

If $P1 \neq P3$ and/or $P2 \neq P4$, then access is denied. Hence, in this example:

If

$$P1 - P3 = 0$$

$$0101 - 0101 = 0$$

or

$$P2 = P4$$

$$P2 - P4 = 0$$

$$3112 - 3112 = 0$$

Access is thereby granted. If

$$P1 - P3 \neq 0$$

or

$$P2 - P4 \neq 0$$

Access is not granted.

Fig. 7 provides a schematic illustration of how P1, P2, UGI#1 and UGI#2 are extracted and compared with P3 and P4.

Therefore, the pre-defined relationship in this example is:

$$P1 - P3 = 0 \text{ and}$$

$$P2 - P4 = 0$$

Where in the description of this embodiment reference is made to the first password, this should be taken to mean variables P1 and P2, whilst the second password is variables P3 and P4 which has been obtained from the

extracted UGI#1 and UGI#2 of the UGI. In other embodiments, only one set of alphanumeric characters could be nominated as the password.

The authentication software 18 determines that the purchase request details entered on form 32 are correct by first reading the Date Stamp "130899-150325" submitted with the UGI data and comparing it with the Date Stamp recorded in the Database 16 to first verify the identity of the person making the purchase request.

As in this embodiment. P1-P3 and P2-P4 is '0', the client user 30 is deemed to be the authentic owner of the Credit Card and the transaction is allowed to proceed as shown in Fig. 5. When a transaction is authorised by the system, a transaction number may be issued to the person making the request to verify the time that the authorisation request has been made.

If either of these two sums had yielded a result that is greater or less than zero, due to a purchase request by the unregistered client user 31, the authentication program 18 determines that the purchase request is not from an authentic card holder or registered user and access is denied as shown in Fig. 6. Authorisation is then declined and the Issuer advised of a possible fraudulent attack against the card

As the above relationship is satisfied, the authentication program sends a message to the server 22 of the Internet vendor 23, that the credit card number is an authorised registered user of the authentication system. The Internet vendor can then ensure that an authorised person is making the purchase request and thereby approve the sale.

Preferably, upon completion of the above steps, the UGI and submitted password residing on the server 14 is destroyed.

The above steps are summarised in Fig. 4.

Step 70

Upon registration, a credit card holder is issued with a UGI and a password which he/she has nominated as shown in Fig. 1B. The password and UGI are used to authenticate a purchase request via the Internet from his/her credit card.

Step 80

The credit card holder submits a purchase requests from a Internet vendor and fills in a virtual form 32 (Fig. 2) which is accessed from an Internet vendor's web site. Upon receipt, this information is routed to the credit card authentication server 14 (Fig 1).

Step 90

The credit card authentication server 14 receives the information routed from the vendor which includes the first password and the UGI.

Step 100

The authentication software 18 is initiated and the first password is stored in the RAM of the server 14.

Step 110

The authentication software 18 then extracts the password embedded within the UGI and the Date Stamp and also stores this in RAM.

The UGI number is then compared on the random table number 20 and the corresponding birth date is then determined from the birthday chart of Fig. 3.

The date stamp from the UGI graphic is compared with the date stamp recorded in the data base 16 to determine if they are matching and thereby identify who the person making the purchase request is meant to be.

Step 120

The first password (P1,P2) of Step 100 is then compared with the second password (P3,P4) from the extracted UGI number of Step 110 (UGI#1.UGI#2) to determine if they are equal.

If they are equal then the authentication program proceeds 18 to step 130.

If they are not equal the authentication program proceeds to step 140.

Step 130

The transaction is authorised and the authentication program verifies that the purchaser's request is made by a registered user of the system as shown in Fig. 5.

Step 140

The transaction authorisation is denied and a message displayed to the person making the request is displayed as shown in Fig. 6. The CCAC 15 then advises the credit card issuing authority that the an unauthorised purchase attempt has been made with the card.

If the relationship does not exist, the transaction is not approved and a GIF graphic "ACCESS DENIED" is posted in the field 44 of form 32 as shown in Fig. 6 from client 30 Internet browser. Approval for the purchase request is not granted and this information is then sent to the server 22 of the Internet vendor 23.

It should also be noted that any relationship may be used to compare the first password (P1,P2) with the second password (P3,P4).

For example, the relationship might be: $y = mx + c$

where y is P1 or P2 and x is P3 or respectively P4 and m and c are constants as shown by the two equations below:

$$P1 = mP3 + c \text{ and/or}$$

$$P2 = mP4 + c$$

Another formula may be $y = mx$.

Although the embodiment described above requires a user to register with the CCAC 15 by filling in the form located on CCAC 15 web site 21, in other embodiments, the user may be required to register the information shown in Fig. 1A first with the credit card issuing authority who will authenticate the user from personal

information held on the database 16 and may obtain the information from their own web site, via a form, or over the telephone. Furthermore, it is preferable that the UGI graphic and the password are not sent in the same email for added security purposes. The embodiment above was shown with the UGI graphic and the password in the one email for illustrative purposes.

It should also be realised that in another embodiment, more than one server 14 may be involved with the credit card authentication centre and furthermore the database and server 16 and server 14 may not be placed in the same location for added security. Additionally, it is preferable that all transactions between the internet vendor and the credit card authentication centre 15 are encrypted.

It is also preferable that any transactions between the client 30...31 and the Internet vendor 23 ... 25 are also encrypted. Additionally, in some embodiments the credit card authentication centre may be the credit card issuing body. It will be realised that the system may be implemented for other security applications such as verifying that a particular authorised user has access to particular computer files.

The client 30...31 shown in this embodiment has been a personal computer having access to the internet. In other embodiments, the client of the computer network may take the form of a mobile phone with WAP capabilities for accessing the Internet. Additionally, the computer network may not be the Internet but could be an organisation's LAN which is used to grant access to particular files.

The UGI graphic is any graphic which is unique and may be created according to the Mandlebrot set, any graphic image or alternatively it could be a thermal image of a person to whom the image is assigned to.

A copy of a UGI and password may be issued to two or more authorised users so that groups within an organisation may gain access to files on the computer network.

The authentication system could be used in embodiments other than for credit card services such as in anti-hacking applications whereby an authorised user is permitted to access files on a server by submitting their issued UGI and password.

The embodiment provides a method and system whereby an Internet vendor is able to authenticate that a person making a purchase request via the Internet is in fact the authentic credit card holder. Because the person making the purchase request must submit both a UGI and a password, this substantially enhances the security of the system rather than using an alphanumeric password on its own which a third party could easily copy.

Other embodiments may require that a new UGI is generated for each registered user over a pre-defined time period, such as on a monthly or annual basis. Furthermore, a number of UGI's may be issued to a registered user in which one of them will be a valid UGI (known to the registered user) and the other UGI's will be fake so as to make it difficult for a fraudster to know which UGI is the correct UGI.

The service request in other embodiments may be for financial transactions such as EFTPOS transactions.

In another aspect, only a UGI without the password could be issued to a person, such as the thermal image of that person referred to above. This thermal image could be used to allow a person to access the computer system as described above without the steps of comparing the password. This would allow a registered user of the system

to gain access to files remotely rather than relying on a password. The UGI submitted by an access request would be compared with one recorded in the database 16 to determine whether a correct UGI has been presented. Should a correct UGI be presented, the person making the request is granted registered user status.

In another embodiment, the service request may be for electronic mail services. In this regard, a client user would prepare an email to be sent to another email account and before sending the email, the client user would submit with the email, the UGI and password in fields created in the client's electronic mail application, such as in Outlook Express™ by Mircosoft Corporation or Lotus Notes™ by Lotus Development Corporation. The email would be routed to the CCAC 15 rather than directly to the recipients email account and thereby authenticated as an actual email from the sender. Once the email is authenticated as being from a registered user, a message could be displayed in the email on presentation to the recipient stating that the email has been verified as authentic by the CCAC 15.

It would be appreciated by a person skilled in the art that numerous variations and/or modifications may be made to the present invention as shown in the specific embodiments without departing from the spirit or scope of the invention as broadly described. The present embodiments are therefore, to be considered in all respects to be illustrative and not restrictive.

Claims

1. A user authentication method to authenticate a registered user of a service over a computer network, the method comprising the steps of:

(a) permitting a client user to request a service from a service provider accessible from said computer network;

(b) requiring the client user to submit at least one first password to the service provider;

(c) requiring the client user to submit at least one unique graphic to the service provider, said unique graphic including embedded second password data;

(d) extracting the second password from said embedded second password data contained within said unique graphic;

(e) comparing the submitted first password and extracted second password to determine if a pre-defined relationship exists between the passwords; and

(f) granting the client user authentic registered user status if said pre-defined relationship exists and providing access to said service.

2. A user authentication method as claimed in claim 1, said method further comprising the step of:

(h) allowing a registered user of said service to select said first password.

3. A user authentication method as claimed in claim 1 or claim 2, said method further comprising the step of:

(i) allowing said user to select an input value;

(j) using said selected input number to index a table to determine a table number; and

(k) using the table number to determine an output number and thereby the second password.

4. A user authentication method as claimed in claim 3, wherein said method comprises the step of randomly mapping input values with output values.

5. A user authentication method as claimed in claim 2, said step (h) further comprising the step of:

(i) issuing said second password once the registered user has selected said first password, said second password issued according to said pre-defined relationship.

6. A user authentication method as claimed in any one of the preceding claims, wherein said pre-defined relationship is determined according to the formula:

$$y = x$$

wherein, y is said first password and x is said second password.

7. A user authentication method as claimed in any one of claims 1 to 4, wherein said pre-defined relationship is determined according to the formula:

$$y = mx$$

wherein said passwords are numerical and y is said first password, x is said second password and m is a constant.

8. A user authentication method as claimed in any one of claims 1 to 4, wherein said pre-defined relationship is determined according to the formula:

$$y = mx + c$$

wherein said passwords are numerical and y is said first password, x is said second password and m and c are constant.

9. A user authentication method as claimed in claim 2, wherein in step (h), said registered user selects one or more calendar dates as a password and step (h) further comprises the step of:

(i) issuing a random number associated with said selected one or more calendar dates and using said random number to identify said registered user.

10. A user authentication method as claimed in any one of the above claims, wherein said service relates to credit card payment facilities or electronic mail services.

11. A user authentication method as claimed in any one of the above claims, wherein said service provider is a credit card payment authorisation service.

12. A user authentication method as claimed in any one of the above claims, wherein said unique graphic a fractal.

13. A user authentication method as claimed in claim 10, wherein said fractal is drawn according to a Mandlebrot set according to the set of values of C for which the series $Z_{N+1} = (Z_N)^2 + C$.

14. A user authentication method as claimed in any one of the above claims, wherein date time stamp data is issued to a registered user when they are issued with the unique graphic and this date time stamp is embedded within said unique graphic.

15. A user authentication method as claimed in any one of the above claims, wherein a transaction number is issued to the registered user for each service request that is granted over the computer network.

16. A user authentication system to authenticate a registered user of a service over a communication network, the authentication system comprising:

server means connected to said communications network having one or more information pages associated with a service provider;

a client device adapted to interface with said server means via said communication network, said client device capable of accessing said one or more information pages to thereby permit said user to submit at least

one first password and at least one unique graphic comprising embedded second password data. to the service provider via said one or more information pages; and

authentication means adapted to interface with said server means to thereby extract the second password from the embedded second password data contained within the unique graphic, and compare the submitted first password and extracted second password to determine if a pre-defined relationship exists between the passwords.

wherein in use. the client user is granted registered user status and is allowed access to said service if said pre-defined relationship exists.

17. A user authentication system as claimed in claim 16, wherein said authentication means allows a registered user of said service to select said first password.

18. A user authentication system as claimed in claim 17, wherein said second password is issued once the registered user has selected said first password, and said second password is issued according to said pre-defined relationship.

19. A user authentication system as claimed in any one of claims 16 to 18, wherein said pre-defined relationship is determined according to the formula:

$$y = x$$

wherein, y is said first password and x is said second password.

20. A user authentication system as claimed in any one of claims 16 to 18, wherein said pre-defined relationship is determined according to the formula:

$$y = mx$$

wherein said passwords are numerical and y is said first password, x is said second password and m is a constant.

21. A user authentication system as claimed in any one of claims 16 to 18, wherein said pre-defined relationship is determined according to the formula:

$$y = mx + c$$

wherein said passwords are numerical and y is said first password, x is said second password and m and c are constant.

22. A user authentication system as claimed in claim 17, wherein said registered user selects one or more calendar dates as a password and a random number is issued that is associated with said selected one or more calendar dates, said random number being used to identify said registered user.

23. A user authentication system as claimed in any one of claims 16 to 22, wherein said service relates to credit card payment facilities or electronic mail services.

24. A user authentication system as claimed in any one of claims 16 to 23, wherein said service provider is a credit card payment authorisation service.

25. A user authentication system as claimed in any one of claims 16 to 24, wherein said unique graphic a fractal.

26. A user authentication system as claimed in claim 25, wherein said fractal is drawn according to a Mandlebrot set according to the set of values of C for which the series $Z_{N+1} = (Z_N)^2 + C$.

27. A user authentication system as claimed in any one of claims 16 to 26, wherein date time stamp data is issued to a registered user when they are issued with the unique graphic and this date time stamp is embedded within said unique graphic.

28. A user authentication system as claimed in any one of claims 16 to 27, wherein a transaction number is issued to the registered user for each service request that is granted over the computer network.

29. A user authentication system as claimed in claim 16 or claim 17, wherein said user to selects an input value and uses said selected input number to index a table to determine a table number, and using the table number to determine an output number and thereby the second password.

30. A user authentication system as claimed in claim 29, wherein said system further comprises randomly mapping input values with output values.

31. A user authentication system to authenticate a registered user of a credit card service in an Internet environment, the authentication system comprising:

server connected to the Internet having one or more web pages associated with said vendor, said vendor web pages permitting purchase of goods/services therefrom;

a client device operable by a user, said client device adapted to connect to said server via the Internet and download one or more of said web pages, said client user being thereby permitted to submit a first password and, a unique graphic including an embedded second password, to the service provider via said web pages; and

authentication software adapted to interface with said server to thereby extract the second password from the unique graphic and compare the submitted first password and second password to determine if a pre-defined relationship exists between the passwords,

wherein in use, the client user is granted registered user status and is allowed access to said credit card service if said pre-defined relationship exists.

32. A user authentication method to authenticate a registered user of a service over a computer network, the method comprising the steps of:

(a) permitting a client user to request a service from a service provider accessible from said computer network;

(b) requiring the client user to submit a unique graphic to the service provider;

(c) comparing said submitted unique graphic with a unique graphic pre-recorded with said service provider to determine if they are the same; and

(d) granting the client user registered user status if said submitted unique graphic is the same as said unique graphic pre-recorded with said service provider and thereby providing access to said service from said computer network.

33. A user authentication method to authenticate a registered user of a service over a computer network, substantially according to any one of the examples described herein with reference to the accompanying drawings.

34 A user authentication system to authenticate a registered user of a service over a communication network, substantially as herein described with reference to the accompanying drawings.

35. A user authentication system to authenticate a registered user of a credit card service in an Internet environment, substantially as herein described with reference to the accompanying drawings.

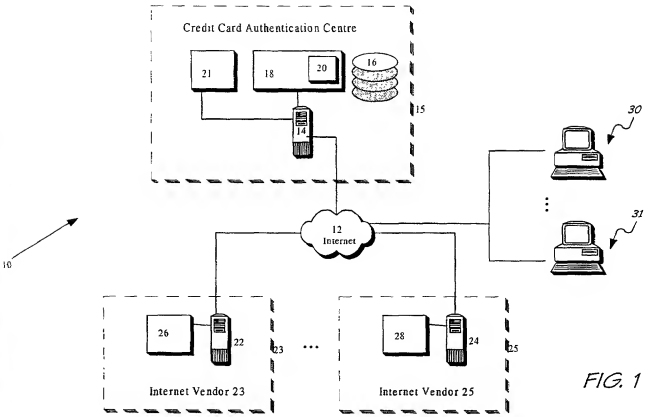


FIG. 1

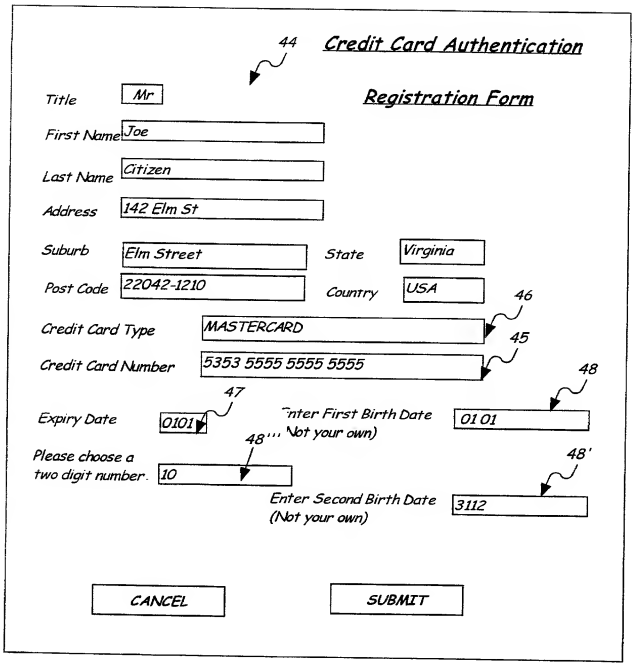

44
Credit Card Authentication
Registration Form
Title
Mr
First Name
Joe
Last Name
Citizen
Address
142 Elm St
Suburb
Elm Street
State
Virginia
Post Code
22042-1210
Country
USA
46
Credit Card Type
MASTERCARD
45
Credit Card Number
5353 5555 5555 5555
48
47
Expiry Date
0101
Enter First Birth Date
(Not your own)
01 01
48'''
48'
Please choose a
two digit number.
10
Enter Second Birth Date
(Not your own)
3112
CANCEL
SUBMIT
43

FIG. 1A

To: Joe_Citizen@hotmail

From: ccas@email.com

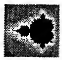
Subject: Registration of credit card service

Date: 13 August 1999

Dear Mr Citizen

We confirm that you have now been registered with our service.

Your Password is: 01013112

Your UGI is Attached: 

Yours sincerely

The Manager

FIG. 1B

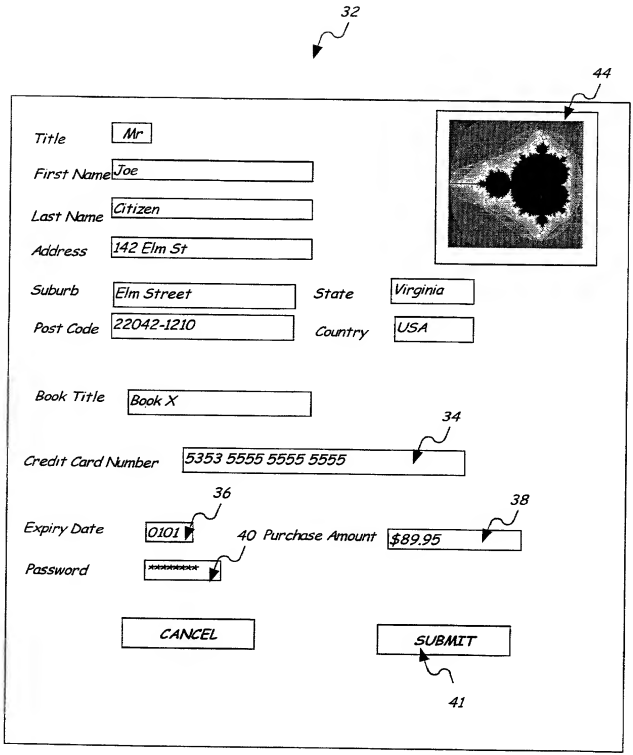


FIG. 2

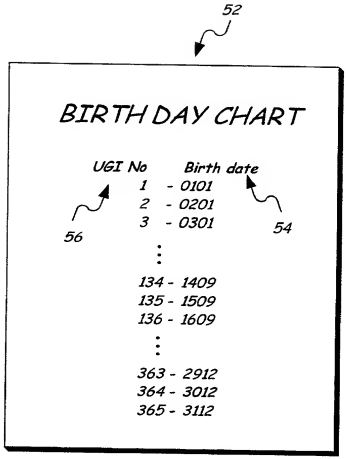


FIG. 3

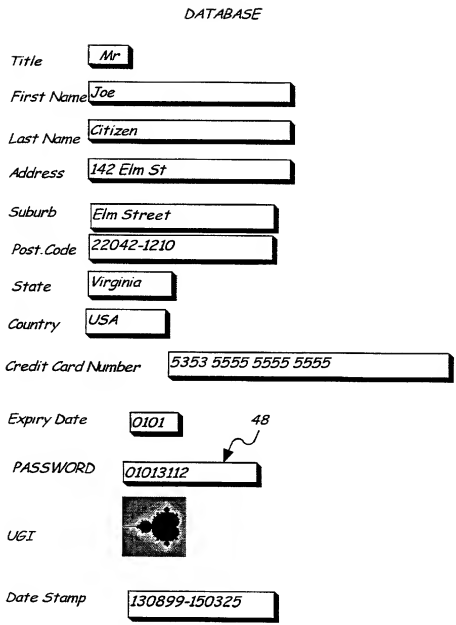

DATABASE
Title
Mr
First Name
Joe
Last Name
Citizen
Address
142 Elm St
Suburb
Elm Street
Post.Code
22042-1210
State
Virginia
Country
USA
Credit Card Number
5353 5555 5555 5555
Expiry Date
0101
48
PASSWORD
01013112
UGI
Date Stamp
130899-150325

FIG. 3A

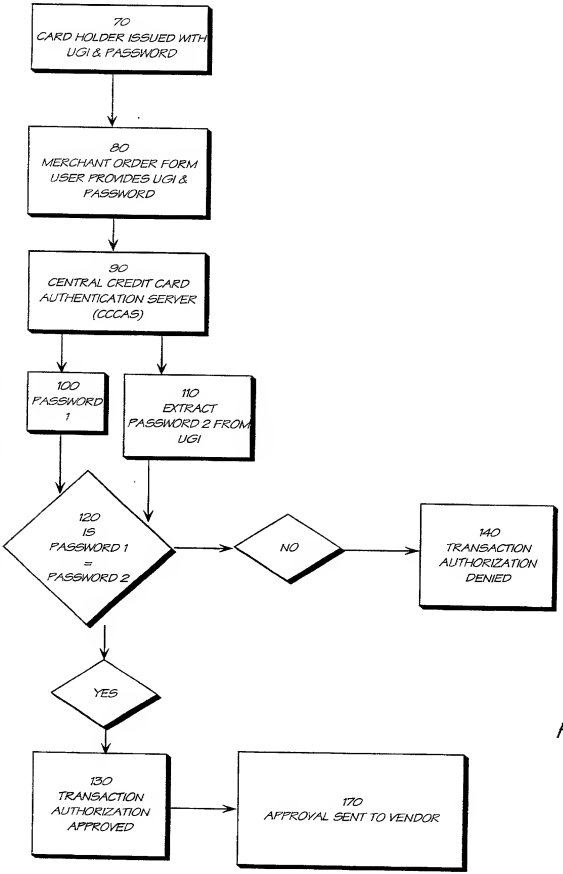

70
CARD HOLDER ISSUED WITH UGI & PASSWORD
80
MERCHANT ORDER FORM USER PROVIDES UGI & PASSWORD
90
CENTRAL CREDIT CARD AUTHENTICATION SERVER (CCCAS)
100
PASSWORD 1
110
EXTRACT PASSWORD 2 FROM UGI
120
IS PASSWORD 1 = PASSWORD 2
NO
140
TRANSACTION AUTHORIZATION DENIED
YES
130
TRANSACTION AUTHORIZATION APPROVED
170
APPROVAL SENT TO VENDOR

FIG. 4

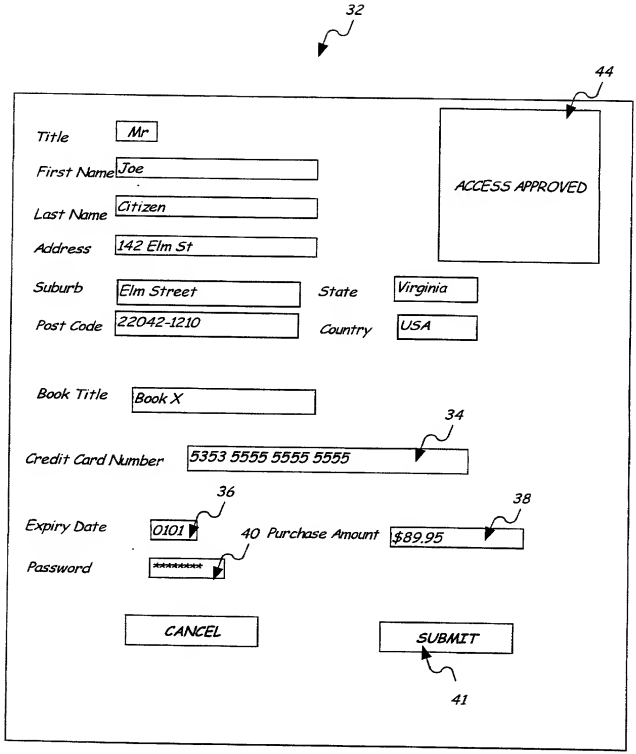

32
44
Title
Mr
First Name
Joe
Last Name
Citizen
Address
142 Elm St
ACCESS APPROVED
Suburb
Elm Street
State
Virginia
Post Code
22042-1210
Country
USA
Book Title
Book X
34
Credit Card Number
5353 5555 5555 5555
36
38
Expiry Date
0101
40
Purchase Amount
$89.95
Password
****
CANCEL
SUBMIT
41

FIG. 5

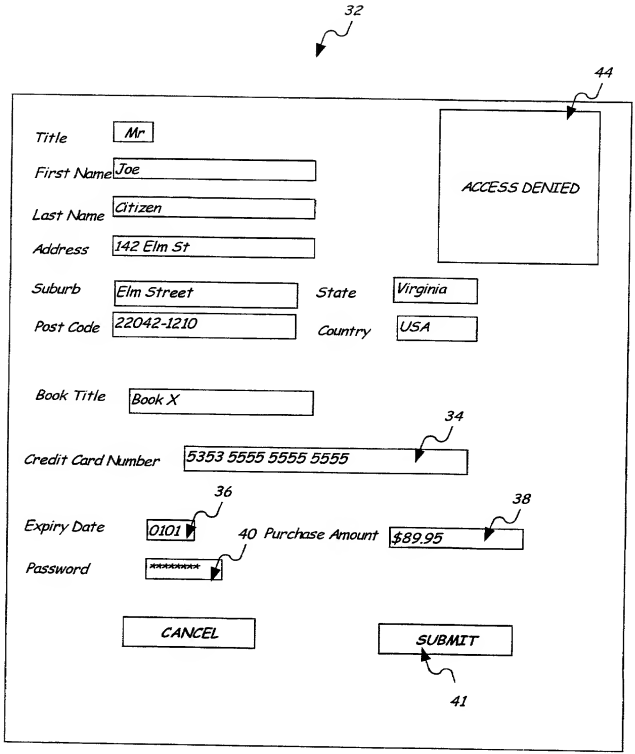

32
44
Title
Mr
First Name
Joe
Last Name
Citizen
Address
142 Elm St
Suburb
Elm Street
State
Virginia
Post Code
22042-1210
Country
USA
ACCESS DENIED
Book Title
Book X
34
Credit Card Number
5353 5555 5555 5555
36
Expiry Date
0101
40
Purchase Amount
38
$89.95
Password
****
CANCEL
SUBMIT
41

FIG. 6

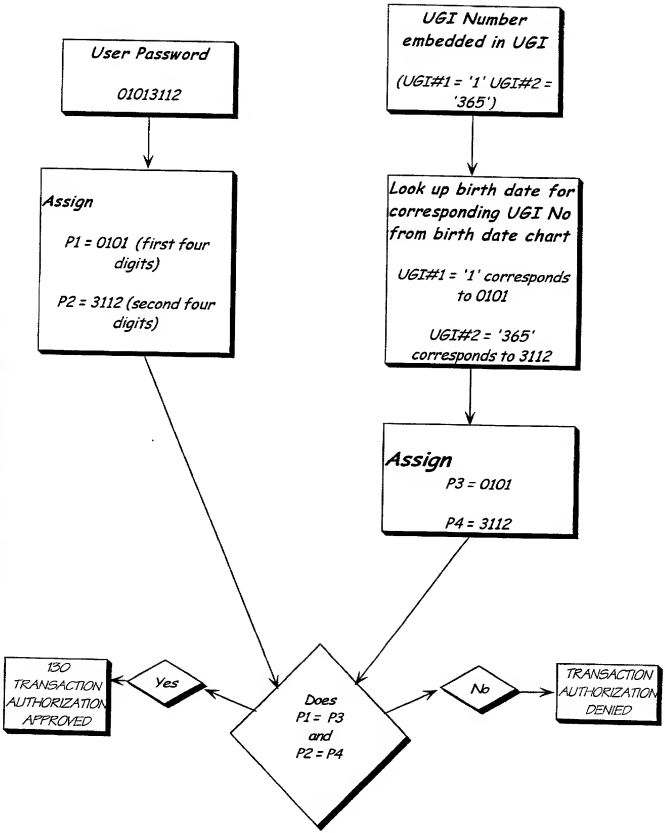

User Password
01013112
UGI Number embedded in UGI
(UGI#1 = '1' UGI#2 = '365')
Assign
P1 = 0101 (first four digits)
P2 = 3112 (second four digits)
Look up birth date for corresponding UGI No from birth date chart
UGI#1 = '1' corresponds to 0101
UGI#2 = '365' corresponds to 3112
Assign
P3 = 0101
P4 = 3112
Does P1 = P3 and P2 = P4
Yes
130 TRANSACTION AUTHORIZATION APPROVED
No
TRANSACTION AUTHORIZATION DENIED

FIG. 7

DECLARATION FOR USA PATENT APPLICATION

(including Design and National Stage PCT) Attorney's Docket ID: _____

As a below named inventor, I hereby declare that:
My residence, post office address and citizenship are as stated below adjacent to my name. I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought

on the invention entitled: USER AUTHENTICATION SYSTEM

the specification of which:

___ is attached hereto.
(or)
___ was filed on _____ was amended on _____ (if applicable), and was filed

as U.S. Application No. or PCT International Application No. _____.

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment specifically referred to above. I acknowledge the duty to disclose information which is material to patentability as defined in 37 CFR 1.56.

I hereby claim foreign priority benefits under 35 U.S.C. 119(a)-(d) or 365(b) of any foreign application(s) for patent or inventor's certificate, or 365(a) of any PCT international application which designated at least one country other than the United States of America, listed below and have also identified below, where priority is not claimed, any foreign application for patent or inventor's certificate, or any PCT international application, having a filing date before that of the application on which priority is claimed. (___ ADDITIONAL APPLICATIONS IDENTIFIED ON ATTACHED SHEET)

Prior Foreign Application No.	Country	Day/Month/Year Filed	Priority *NOT* Claimed
PQ2184	AUSTRALIA	13.08.1999	—
PQ2347	AUSTRALIA	23.08.1999	—

I hereby claim the benefit under 35 U.S.C. 120 of any U.S. application(s), or 365(c) of any PCT application designating the U.S., listed below; and insofar as the subject matter of each of the claims of this application is not disclosed in the prior U.S. or PCT application in the manner provided by the first paragraph of 35 U.S.C. 112, I acknowledge the duty to disclose information which is material to patentability as defined in 37 CFR 1.56 which became available between the filing date of the prior application and the national or PCT filing date of this application. (___ ADDITIONAL APPLICATIONS IDENTIFIED ON ATTACHED SHEET.)

U.S. or PCT Parent Application No.	Parent Filing Date (Day/Month/Year)	Parent Patent No. (if applicable)

As a named inventor, I hereby appoint the registered practitioners of LARSON & TAYLOR associated with Customer Number 000881 to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith. Direct all correspondence to that Customer Number.

000881

Direct all telephone calls to _____ at TEL (703) 739-4900 (Fax: 703-739-9577) E-Mail: _____

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under 18 U.S.C. 1001 and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

SOLE OR FIRST INVENTOR	
Given Name (first and middle [if any])	Joseph Elie
Family Name or Surname	TEFAYE
Full Post Office Address	63, Wood Street, Templestowe, Victoria 3106, Australia
Residence - City, State/Country (if different from P.O. address)	
SIGN AND DATE HERE: Inventor's Signature:	Date: FEB 11 2002
Citizenship	AUSTRALIAN

SECOND JOINT INVENTOR (if any)	
Given Name (first and middle [if any])	
Family Name or Surname	
Full Post Office Address	
Residence - City, State/Country (if different from P.O. address)	
SIGN AND DATE HERE: Inventor's Signature:	Date:
Citizenship	

THIRD JOINT INVENTOR (if any)	
Given Name (first and middle [if any])	
Family Name or Surname	
Full Post Office Address	
Residence - City, State/Country (if different from P.O. address)	
SIGN AND DATE HERE: Inventor's Signature:	Date:
Citizenship	

FOURTH JOINT INVENTOR (if any)	
Given Name (first and middle [if any])	
Family Name or Surname	
Full Post Office Address	
Residence - City, State/Country (if different from P.O. address)	
SIGN AND DATE HERE: Inventor's Signature:	Date:
Citizenship	